Fortify Scan Issue: Code broken into a large number of FPR files

⚠ **This page has been made public for vendors**

Question

What does the Fortify scan issue "Code broken into a large number of FPR files" mean, how can I detect it, and how can I fix it?

Answer

This scan issue indicates that a large number of FPR files were included in the code review package and it may be possible to scan the code to produce fewer FPR files. Fewer FPR files have a number of advantages, including better scan results as Fortify can better detect dataflows through the code, easier to scan, easier to audit, and easier to review.

How to detect

Most applications can be scanned as a single FPR file. Some applications may need to be broken up into multiple scans if the application consists of multiple executables, libraries, or other separate components. However, if the code is broken up into too many scans, say 20, 30, 40, or 100 or more, there is likely a problem with how the code has been divided up. Another sign that the code has likely been divided into too many separate scans is if each scan only includes only a few files.

How to resolve

Review the scan breakdown of the code and try to adjust the scans so fewer are needed to cover the codebase. See if the scans are done by executable. Also consider if the scans can be done at a level higher in the build tree. If it is possible to consolidate the scans, please do so.

If it is determined that there is no reasonable way to consolidate scans, please include a readme file along with the V&V secure code review package that explains why this breakdown is necessary.

References

- **VA Top 10 Fortify Scan Issues For 2016 (Q4)**
- **VA Top 10 Fortify Scan Issues For 2016 (Q3)**

HPE Fortify Version	16.11 and later
Programming Language	☑ C/C++ ☑ .NET ☑ Java ☑ Objective-C ☑ Other
Fortify Audit Workbench	☑ Yes ☐ No
Fortify IDE Plugin	☑ Yes ☐ No
Other Fortify Component	☑ Yes ☐ No

Request code review tools, validations, and support HERE.